# Integrated Technologies to Enable DAT

**Antonello Mangogna**
Via Europa
20014 Nerviano (MI)
ITALY

antonello.mangogna@galileoavionica.it

## *ABSTRACT TITLE*

*An effective process of defence against terrorist actions starts from a surveillance system which is reliable in the information produced and the continuity of the service, capillary in diffusion and coverage of spaces which represent a potential incursion scenario, affordable in terms of installation, operation and maintenance costs.*

*The reference surveillance scheme considered consists of three cooperative segments as a minimum, each one composed by a specialised surveillance network.*

*The first segment is relevant to air networks, operating on regional and metropolitan extended areas. The network nodes are represented as Data-Fusion nodes (DFN) equipped with sensors and capable of processing and exchanging data with other nodes in the network. The interconnection gives the system the ability to individuate appreciable targets with a high level of confidence by means of sensor fusion techniques.*

*The second segment is represented by territorial networks on urban scale, composed of DFN equipped with miniaturized sensors, reachable and controllable through civil communication infrastructures. Sensors' detection capability ranges from nuclear, bacteriological and chemical agents to the detection of the transit of suspect individuals and objects across pre-defined areas.*

*The third segment, located close to individuals transit and points of exchange, refers to the use of RFID tags which allow immediate and automated identification of goods traffic, thus allowing selective interventions with respect to safety and reserve criteria.*

## FOREWORDS

Terrorism, is used to be perceived as a diffuse risk, has now become a central threat for our open societies and a core security preoccupation in every State.

Countering terrorism is a major goal of nations at this time. Terrorism threat changes as anti-terrorism activities evolve. Conventional attacks have been the predominant methods so far, while chemical, biological, radiological, or nuclear weapons attack could be expected in the near future.

Generally, terrorism attacks are targeted toward infrastructural systems or toward individuals' health: difficulty to provide infrastructures' and individuals' security is mainly related to the asymmetry of rules between nations and terrorists. The goal of ensuring **fairly and truly effective protection** to individuals by limiting restrictions to personal liberty, could appear as weakness of nations in fighting terrorism

Mangogna, A. (2006) Integrated Technologies to Enable DAT. In *Tactical Decision Making and Situational Awareness for Defence Against Terrorism* (pp. 16-1 – 16-10). Meeting Proceedings RTO-MP-SCI-174, Paper 16. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **01 MAY 2006** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Integrated Technologies to Enable DAT** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Via Europa 20014 Nerviano (MI) ITALY** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADM202346., The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **10** | |

attacks. Indeed, this is widely accepted as the key to cope with attempts of making individuals frightened and weakening democratic institutions, through damaging their essential or strategic interests.

An effective process of settling an valuable infrastructural security system against terrorist attack relies upon surveillance system which is reliable in the information produced and the continuity of the service, capillary in diffusion and coverage of spaces which represent a potential incursion scenario, affordable in terms of installation, operation and maintenance costs.

Besides, a security system – providing a holistic picture of the scenario – will better support TDM and therefore deployment against threats.

Scope of the paper is to describe technologic solutions supporting implementation of cooperative nodes the security surveillance network will consist of.

Such data-fusion nodes are intended to provide the functions required to improve **Situational Awareness** of the security scenario through an **Automated Information Process** generating those **cognitive aids** required to depict a synthesised view of the operational environment.

Focus onto so-called data-fusion nodes will be provided in terms of expected functions and **maturity** of enabling **technologies**.

## SURVEILLANCE NETWORKS SYSTEM AND SITUATIONAL AWARENESS

In order to guarantee a pervasive and effective coverage of sensitive scenario, the reference surveillance system considered in this paper consists of three cooperative segments at least, each of them composed by a specialised surveillance network:

- The first segment is relevant to air-network that operates over regional – both sea and land – and over metropolitan-extended areas.
- Territorial network on urban scale represents the second segment. It works at quarter and building level, including transportation systems.
- The third segment, at gate-level, is located close to passage of individuals and goods.

### Air-segment network

The network nodes could be physically represented by remotely driven platforms (like UAVs), capable of acquiring data, perform a computational treatment and then exchanging data with other nodes, also through intermediate nodes that will act as switching units. Remote command and control centres are part of such network.

Each node in the network is equipped with a data-fusion engine consisting of a suite of sensors able to capture information from the field that can be further processed to detect any event significant with respect to security objectives.

At the air-segment [ASN] of the surveillance network, imagery-only sensors are those effective towards awareness objectives. They can be either visible or electro-optical cameras or even Multi-spectral or Hyper-spectral sensors all providing imagery information of the monitored area. In such a case the sensor-fusion engine will combine the information of all the sensors to improve the reliability of the overall target acquisition process.

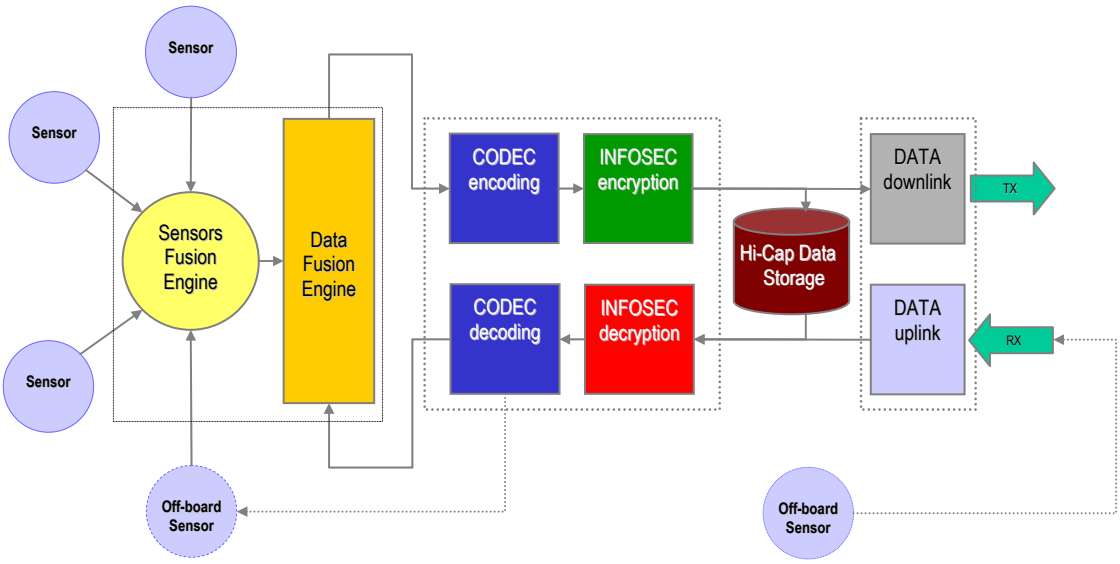


**Figure 1: Data fusion Node – Block Diagram**

### Sensor Fusion Engine

Upon completion of a preliminary study about this topic, GA is going to settle some working groups to further develop capabilities in the sensor-fusion domain. Stating that experience of GA is mainly settled onto IR, IRST, RADAR and other sensors, the following working groups are going to be address:

- IRST-RADAR fusion
- IR- Image mode RADAR fusion
- IR-SWIR fusion
- Panchromatic – Hyper-spectral fusion

*IRST-RADAR fusion WG*

The scope of this WG is to finalise methodologies to fuse such sensors' output with the aim of achieving higher performances into detection, search and track of targets. Actually, the combination of the two sensors should join the precision of RADAR in the target's distance measurement and the angular precision (direction) of an IRST sensor: the expected result is a higher resolution when tracking the target.

Further improvements are expected in classifying the target: a higher precision of the distance can improve the interpretation of IR image, while combination of IR and ISAR images can improve the confidence in target recognition process.

*IR - Image-mode RADAR fusion WG*

The scope of this WG is to finalise fusion of SAR/ISAR images with IR ones. Since the two domains considered provide complementary data, an improvement is expected into classification of the target and in the resolution of represented scene as well.

*LWIR-SWIR fusion WG*

The goal of this WG is to define and implement **real-time** algorithms in order to fuse images coming from SWIR and IR cameras.

The reference block diagram of a sub-system integrating IR and SWIR cameras for image fusion purpose is shown in the figure below.

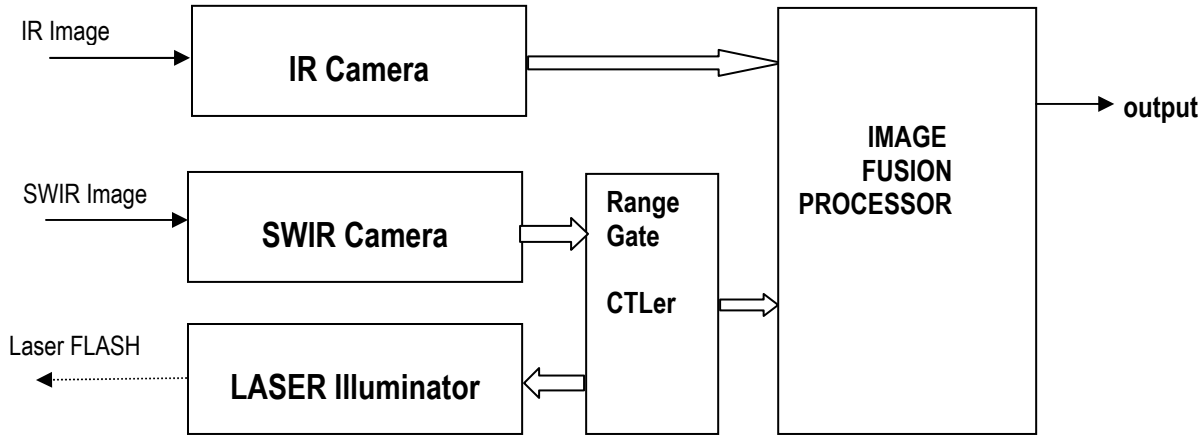


**Figure 2: SWIR/IR sensors assembly for image fusion purpose**

Further processing techniques will be focused towards:

- Objects detection in the scene (LWIR/MWIR band),
- Classification and identification (SWIR/Range Gated),
- Image fusion
- Automatic tracking of targets

The following figure shows the result of an off-line image fusion of SWIR and LWIR cameras.

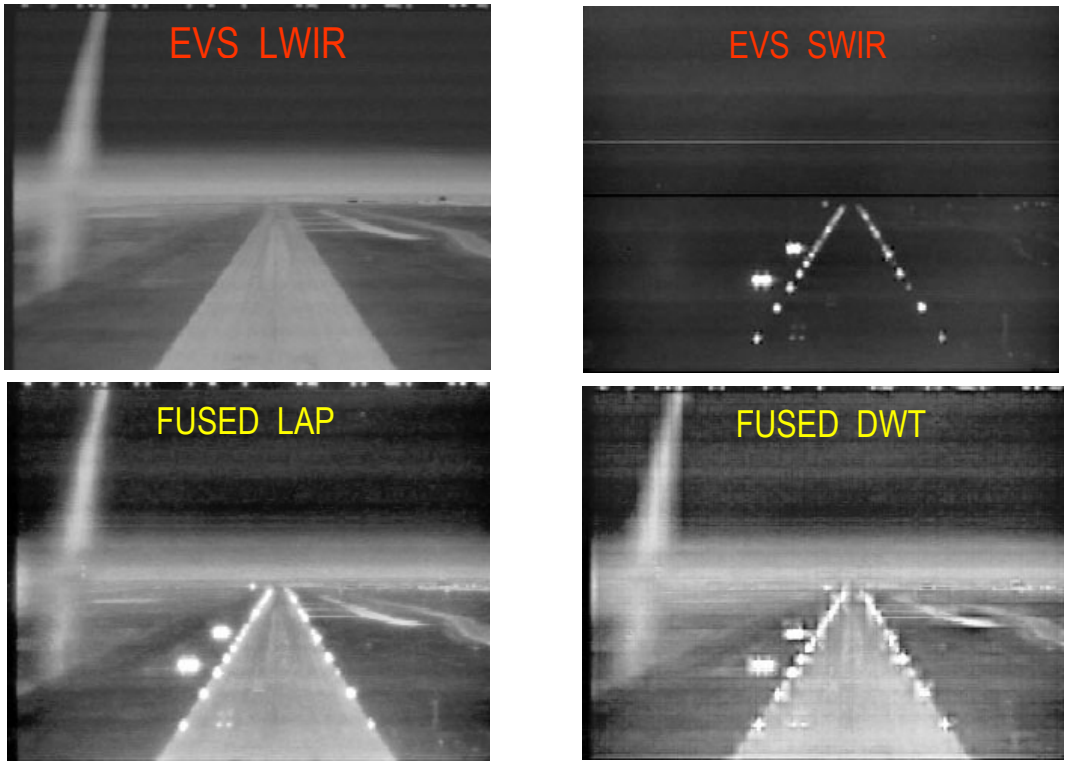


**Figure 3: Example of off-line image fusion of LWIR (8-12μm) and SWIR (1-2μm) cameras**

*Panchromatic – Hyper-spectral WG*

The scope of this WG is to finalise methodologies to fuse such sensors' output to enhance detection, search and tracking performances as they are provided when not fused.

Since resolution of panchromatic images is much more than M/S and hyper-spectral images can provide, a technique used to merge such images is the image-fusion. Other techniques providing the expected improvements are *data merge and band sharpening.*

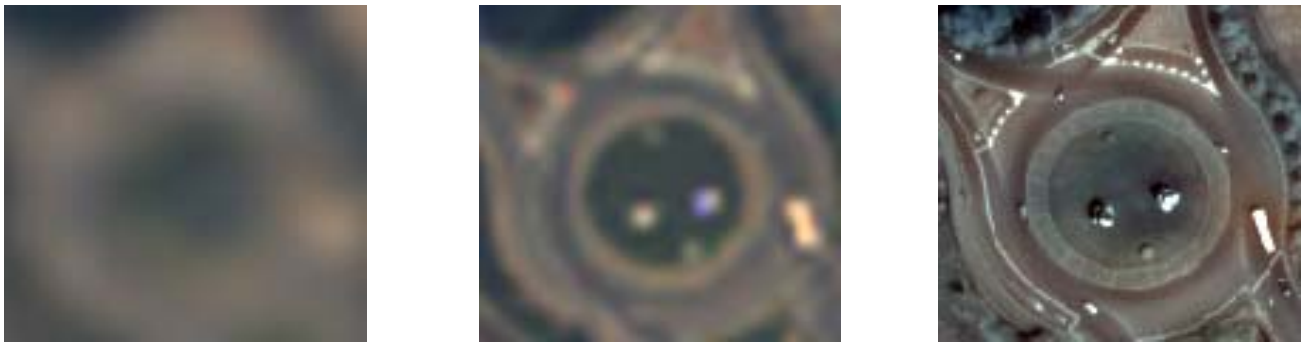

**Figure 4: Example of off-line image fusion of PAN and M/S images**

**Data fusion engine**

Once the **sensor-fusion** engine has provided a reliable representation of the monitored area, the **data-fusion** engine will intervene to synthesize a representation of objects and events that are significant with respect to security objectives. Since the sensor-fusion process cannot avoid misinterpretation in the target detection, an **automated process** is required to minimize probability to generate false alarms: verification and analysis of data acquired is necessary before any catastrophic measures may be taken in response to any sensor detection.
Further, the data-fusion engine may combine data acquired from monitored area and information coming from remote nodes through the network, in order to make more robust the detection, classification and identification process of threats.
Methodologies have been identified for **automated processing** of the alarms: they can be implemented into a **decision support system** composed of a rule-based expert system, having a **knowledge base** and a **non-deterministic inferential engine**.

**Non-deterministic Inferential engine as basis of data-fusion processes**

The expert system is a program the data-fusion node run to determine facts from data coming from observation of the outdoor environment, by using a set of flexible rules stated in the base of knowledge. The inferential engine is the key element to determine those facts: it is non-deterministic since even lack of completeness of knowledge base doesn't prevent it to formulate hypothesis and make assumptions useful to complete the decisional process. Facts determined through this inferential process are fed to knowledge base. The same data the sensors draw from the scenario, weighted upon a different base of knowledge leads to a different decision: for this reason the inferential engine is called non-deterministic.

The main goal of such a data-fusion process - based on a non-deterministic inferential engine – is to improve and validate information sourced from the sensors involved.

**Network operability of DFN**

Upon data-fusion engine has determined facts that are relevant to the surveillance process, information is forwarded to the network – through radio data-link – to enhance the situational awareness of the observed area. Besides, when required to operate silently, nodes may acquire data and securely store them aboard. Later, they will forward information locally acquired/stored to the network.

When received in the destination node, data coming from remote DFNs are fed to the local knowledge base with the aim to better support automated decision support at these nodes too. Security of exchanging data is guaranteed by encryption mechanism provided in the DFN, along the forwarding path to the network.

In order to guarantee interoperability among nodes, amount of data to be forwarded to the network has to be minimized: that is the key factor of surveillance system effectiveness. At this purpose, the DFN provide compression mechanism to the data-stream with dedicated CODEC.

GA has settled a WG with the goal to develop technology of CODEC for such a kind of application.

The aim of this WG is to develop a class of CODECs allowing data-exchange over any communication channels, with small bandwidth requirement.

CODECs that are going to be developed will be asked to allow real-time operation on the basis of imagery acquisition even from remote sensors, i.e. located onto remote nodes of the network.

The main characteristics expected for the class of CODECs GA is going to develop are as follows:

- Error Resilience: it's the real-time capability of the CODEC to detect and/or correct errors
- Security: it's the CODEC's capability to implement encryption and decryption of processed data-stream to guarantee secure data handling;
- Scalability: it refers to the user's opportunity to select the appropriate rate of compression with respect to the communication channel's bandwidth. The selection of the compression rate (having the twofold meaning of loss rate) is expected to be an adaptive parameter of the CODEC's configuration;
- Region Of Interest [ROI]: It's another interpretation of scalability. Data-stream can be heavily compressed with the exception of the Region Of Interest, for which the compression level of quality has been kept as high as possible.

### Air-segment network over the sea

Surveillance of sea areas can be implemented at air-segment level by using DFN (Data-Fusion Nodes) equipped with sensors like SAR and IRs.

Besides reconnaissance, surveillance and targeting, Synthetic Aperture RADAR can be used for a wide variety of environmental applications, such as monitoring of oil spills and detection of other contaminant fluids on the sea surface.

This application can be useful to detect attacks with contaminants at shores where resorts are located with thousand of bathing people.

### Territorial-segment network

The second segment of the surveillance network is composed of data-fusion nodes as well, although carried and deployed in accordance with indoor surveillance requirement.

DFNs that are intended for Territorial-segment Network (TSN) employment, have the same structure of that ones used for ASN (Air-segment Network). Actually, they require to be arranged with a different set of sensors to nearly detect threats like contaminants, explosives, etc.

Further, the DFN will provide a well-suited expert system implementing an inference model dedicated to the territorial environment. Interconnection of DFN whit the network will be guaranteed through a data-link that exploits those communication infrastructures available at territorial level.

As far as the sensor are concerned, along with imagery class of sensors (visible and IR cameras) a new class of sensors come into, to face Chemical, Biological, Radiological and Nuclear (CBRN) threats. The rising technology in this field is the DNA micro-array.

A DNA micro-array (also commonly known as gene chip, DNA chip, or biochip) is a collection of microscopic DNA spots – arranged through an array - grown onto and attached to a solid surface, such as glass, plastic or silicon chip. Thousands of DNA probes can be fitted in a single DNA micro-array. Such probes are being specialized with the attack agent it would be detected: probes sensitive either to carbonchio (anthrax) or to other chemicals agents can be synthesized to early detect the presence of potential attack nearly the sensor's position.

Data coming from CBRN sensors give false alarms. In order to prevent them, once again an expert system, running in the data-fusion engine, will provide the level of verification expected before raising alarms to the network. A specific knowledge base has to be developed for this kind of application.

**Gate-level segment**

The third segment of the surveillance network can be considered as part of the territorial segment since it works in the same environment, but it is focused to control passages between areas having different levels of sensitivity, i.e. boarding gates at the airport, trains, theatres, sports stadium, etc.

To support security operation at this level, the RFID technology is the most likely to be used for.

A RFID identification system consists of three parts:

- A scanning antenna, that can located in a fixed position at the check-point (gate)
- A transponder tag - that has been programmed with information and it's worn be the person who passes through the gate
- A transceiver with a decoder to interpret the data that will be part of the DFN assigned to the checkpoint.

The scanning antenna emits a radio-frequency signal in a short range. The RF radiation constitutes a means of communicating with the transponder tag (the RFID chip) and it provides the RFID (passive) device with the energy to communicate.

When an RFID tag passes through the field of the scanning antenna, by detecting the activation signal: that *wakes up* the RFID chip that will transmit the information on its microchip to the scanning antenna.

RFID tags can be read even in those circumstances, where barcodes or other optically read technologies are useless. The tag need not be on the surface of the object. The read time is typically less than 100 milliseconds and large numbers of tags can be read at once rather than item by item.

This last feature makes RFID technology attractive for the purpose to identify and/or locate a person without it pass through a gate. In such a case, a handheld antenna can be used along with a portable DFN while this DFN is wireless connected to the territorial segment of the surveillance network.

RFID terminal allow to control, in real-time, the identity of all the people entering the gate, without creating delays and queues to access the area. People are only asked to carry along an identification tag that can be read by the RFID system to access personal data that have been stored into.

RFID identification tag can be active as well, so passage through the gate can be stored in the tag to allow further tracking opportunity for the surveillance system.

It's bound that data in the identification tag have to be encrypted for security reason and also to prevent it to be counterfeit.

In addition of RFID, gate-check have to include sensors able to detect the presence of metals, explosives or contaminants, although the positive identification of all the people entering the gate should discourage any attempt to introduce objects to be used for attack.

## *Conclusion*

Situational awareness can benefit from an effective surveillance system, distributed in a pervasive way over the region to control. Sensors are available to detect a large class of threats and automated processes to support decision are coming.

Sensors' effectiveness can be improved through sensor fusion methodologies; while validation of the alarm has to be performed through expert systems that constitute such decision support systems required to improve effectiveness of defence against terrorism attack.
Technology is mature enough to start implementation of the concepts contained in this paper. Flexibility of the DFNs is the key factor to allow further technology insertion, as it will be as mature to be effectively applied.

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| ASN | Air-Segment Network |
| CBRN | Chemical, Biological, Radiological and Nuclear |
| DAT | Defence Against terrorism |
| DFN | Data Fusion Node |
| IR | Infra-Red |
| IRST | Infrared Search and Track |
| LWIR | Long Wavelength IR |
| RFID | Radio Frequency IDentification |
| SA | Situational Awareness |
| SAR | Synthetic Aperture RADAR |
| SWIR | Short Wavelength Infrared Radiometer |
| TDM | Tactical Decision Making |
| TSN | Terrestrial- Segment Network |
| WG | Working Group |
| GA | Galileo Avionica – a FINMECCANICA Company |